DEFENSE INFORMATION SYSTEMS AGENCY

JOINT INTEROPERABILITY TEST COMMAND
INDIAN HEAD, MARYLAND

COMMON ACCESS CARD MIDDLEWARE TEST PLAN

Pub Nr: 4M01.001
DECEMBER 2001

(This page intentionally left blank.)

TABLE OF CONTENTS

Page

APPENDICES

LIST OF FIGURES

LIST OF TABLES

(This page intentionally left blank.)

SYSTEM FUNCTIONAL DESCRIPTION

The Department of Defense (DOD) Access Card Office (ACO) issued smart card requirements for the procurement of middleware to function with the Common Access Card (CAC). The procurement will be executed by the Department of the Navy (DON) Enterprise License vehicle to provide an acquisition means for all Services and Components within DOD.

The CAC has been issued to 140,000+ personnel within DOD with the intent to issue 4.3 million CACs within DOD by mid 2003. Card issuance is accomplished via the DOD Real-time Automated Personnel Identification System (RAPIDS), a computer system with over 1500 identification card issuance stations worldwide. These systems presently use middleware and readers, integrated into RAPIDS, to provide a secure issuance environment.

The middleware support the workstation client requirements of the DOD Components (Army, Navy, Air Force, Marines, and Agencies) to utilize the CAC. The estimates of total license requirements within the Department are 1.5-2.0 million copies. The term *"middleware"* is defined as a specific standards-based software and/or Application Programming Interface (API) that allows a software application running on a device (card) to communicate with the Integrated Circuit Chip (smart card) to read, write and transfer objects (e.g., Public Key Certificate Standards PKCS#11 formatted information objects such as Public Key Infrastructure x.509 certificates, or DOD and Service data containers consisting of binary digits).

TEST BACKGROUND

The DOD ACO, Defense Manpower Data Center tasked the Joint Interoperability Test Command (JITC), Washington Operation, to test smart card middleware for their new Common Access Card (CAC). The JITC will test the middleware for interoperability (technical information exchanged) and compatibility. The middleware must perform their functionality in accordance with the CAC Release 1.0 Middleware Requirements version 2.1 dated December 5, 2001. CACs to be utilized within the test contain an integrated computer chip and will be pre-loaded at the DOD Real Time Automated Personnel Identification System (RAPIDS) work station with the card's requisite, onboard software data containers (PKI certificates, and DOD and Component data).

TEST PURPOSE

To determine middleware compliance to CAC Release 1.0 Middleware Requirements.

REQUIREMENTS

Mandatory CAC test requirements are stated in the ACO CAC Release 1.0 Middleware Requirements, Version 2.1 document dated December 5, 2001. Critical CAC interoperability and compatibility requirements from the standard are expressed within Table 1.

Table 1. CAC Release 1.0 Middleware Test Requirements.

REQUIREMENTS	METHOD OF TEST	MEASURE OF SUCCESS
Encrypt E-mail via DOD PKI Certificate	Operator at keyboard	E-mail successfully encrypted per standard
Decrypt E-mail via DOD PKI Certificate	Operator at keyboard	E-mail successfully decrypted per standard
Digitally sign E-mail and document	Operator at keyboard	E-mail successfully digitally signed per standard
Provide for PIN change in accordance with NSA Regulation (6-8 digit numeric only)	Operator at keyboard or via assistance of RAPIDS station operator	PIN successfully changed and process used in accordance with NSA Regulation (6-8 digit numeric only)
Access, read, and provide to applications the DOD data container	Operator at keyboard- Validation accomplished by a Defense Manpower Data Center application that can view all DOD data written to the card	DOD data container accessed, read, and provided successfully to the applications per standard
Access, read, and provide to applications the Component Specific Area data container	Operator at keyboard - Validation accomplished by testing the developed "Backwards Compatibility" application	Component specific data container accessed, read, and provided successfully to the applications per standard

LEGEND:
CAC – Common Access Card
DOD – Department of Defense
NSA – National Security Agency
PIN – Personal Information Number
PKI – Public Key Infrastructure
RAPIDS – Real-time Automated Personnel Identification System

SCOPE

The JITC will test the CAC middleware at its IA Test and Evaluation Laboratory (IA T&E Lab) at Indian Head, Maryland. Testing will be confined to the JITC IA T&E Lab using host computers (Windows and Unix) and an Ethernet network. This architecture is similar to the DOD operational environment where the CAC middleware might be deployed. Figure 1 shows the CAC baseline operational configuration. Appendix B is the JITC test configuration.

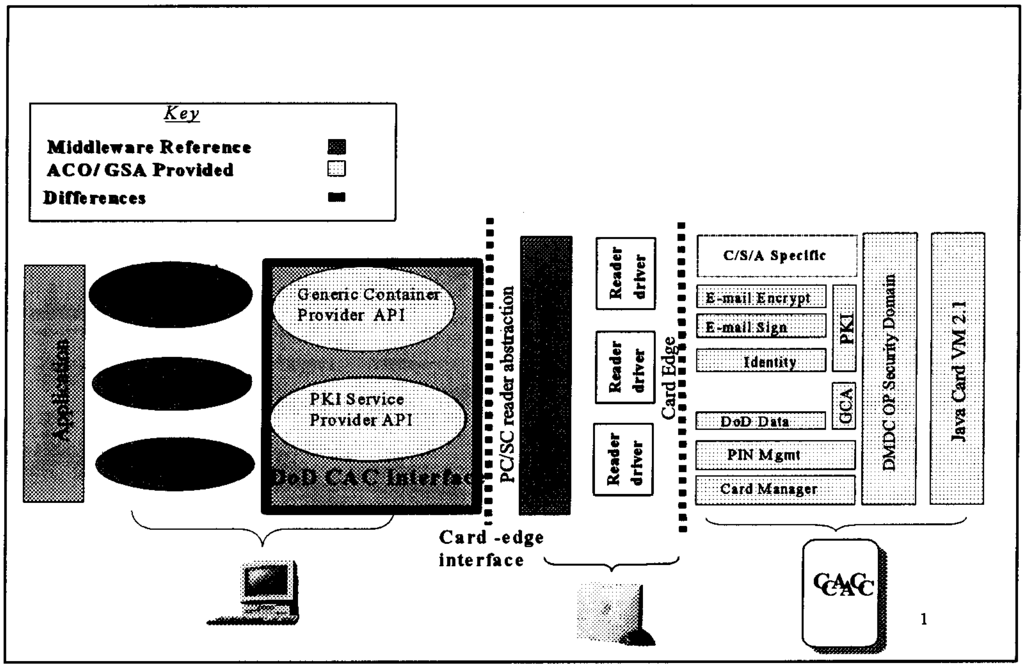

Figure 1. CAC Baseline Operational Configuration

OBJECTIVES AND METHODOLOGY

Determine the extent to which the middleware meets the middleware requirements as defined in the CAC Release 1.0 Middleware Requirement.

> Methodology: The tester will perform routine operations (encryption and decryption), utilizing the card's onboard software (PKI certificates, digital signature, and DOD and Component data container software) to investigate the middlewares characteristics in relation to the CAC middleware requirements
>
> Evaluation: Does the middleware characteristics meet the mandatory requirements (see appendix D).

The JITC will test the middleware on a variety of vendor-specific readers to determine interoperability and compatibility issues using normal, workstation commercial products. Commercial products supplementing the test include Microsoft Word, Outlook and Outlook Express, and Netscape Navigator (all as a basis for operator functionality). Testing will occur both within a common "specific suite" of manufacture's products (card, reader and middleware from the same vendor) and among a disparate collection of different vendor products (varying combinations of card, reader and middleware from different vendors). The CAC test environment will include both Unix and Windows operating system platforms (if applicable), all operated within a distributed Ethernet network environment hosted within the JITC Information Assurance Test and Evaluation Laboratory, Indian Head, Maryland.

PRESENTATION OF RESULTS AND ANALYSIS

The JITC test report will present the final test results, recommendations, and lessons learned in a brief test report card format (see appendix D).

APPENDIX A

ACRONYMS

ACO	Access Card Office
CAC	Common Access Card
DOD	Department of Defense
DODD	Department of Defense Directive
GHZ	Gigahertz
IA	Information Assurance
JITC	Joint Interoperability Test Command
MHZ	Megahertz
NIST	National Institute of Standards and Technology
NT	New Technology
NVM	Non-Volatile Memory
ORD	Operational Requirements Document
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PM	Program Manager
PMO	Program Management Office
RAPIDS	Real-time Automated Personnel Identification System
SP	Service Pack

APPENDIX B

TEST CONFIGURATION

TEST PERSONNEL. Common Access Card (CAC) middleware testers will consist of two person test teams. Testers will generate the test using standard Defense Information Systems Agency network hardware and software configuration items.

TEST CONFIGURATION. Testers will operate all computers through an Ethernet 10BaseT hub to the other laboratory test computers. Figure B-1 shows the test configuration.

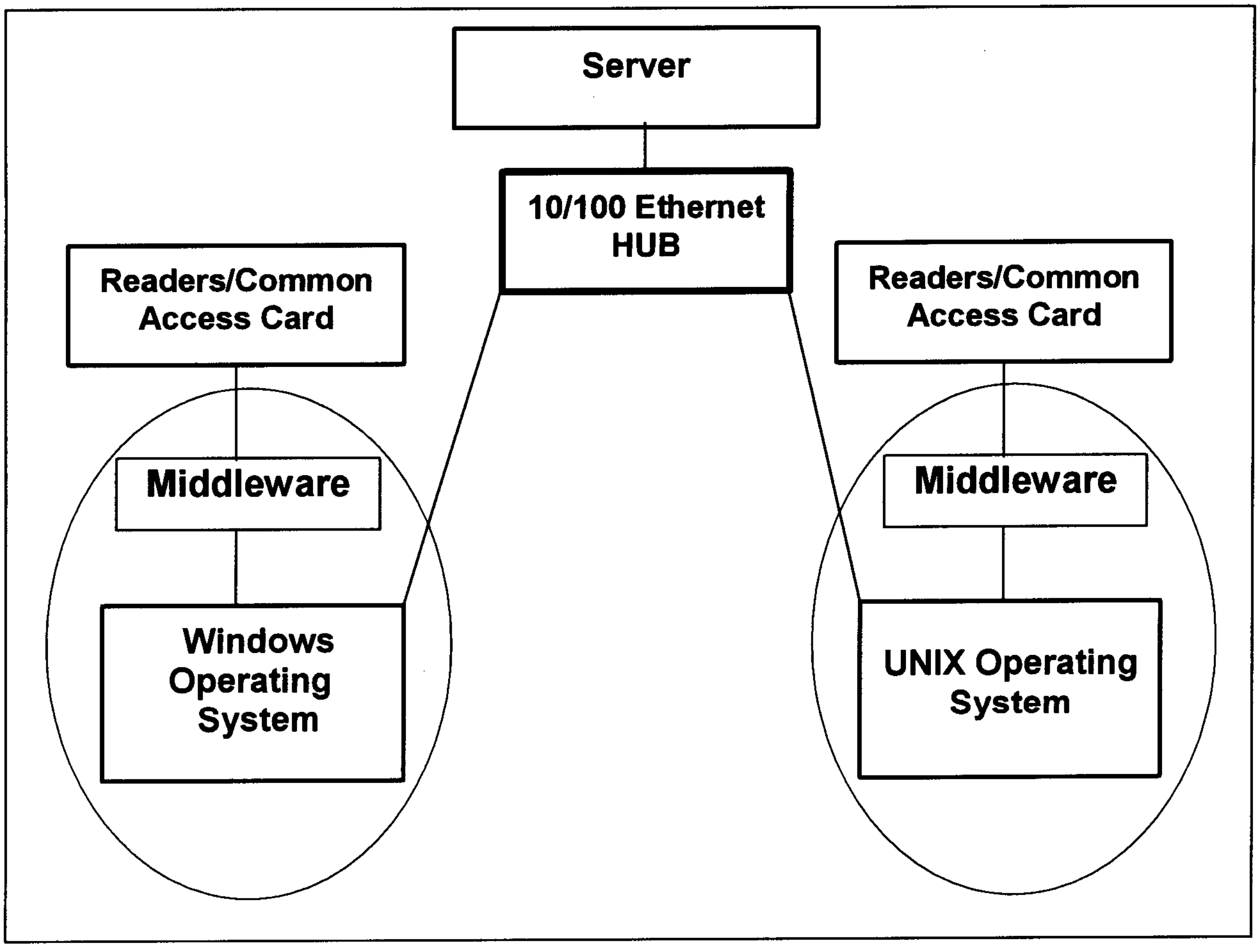

Figure B-1. CAC Middleware Test Configuration

Note: All hosts and network systems will be connected via a 3Com 8 Port, 10BaseT Ethernet Hub, Model 3C1670.

TEST EQUIPMENT. Table B-1 shows the CAC middleware test equipment.

Table B-1. CAC Middleware Test Equipment

OPERATING ENVIRONMENT	PROCESSOR	RANDOM ACCESS MEMORY	DISK (SIZE/INTERFACE)	TYPE NETWORK INTERFACE
Windows 95b	1 GHZ	128 MB	10 GB	10/100
Windows NT 4.0 SP 6.0a	1 GHZ	128 MB	10 GB	10/100
Windows 2000	1 GHZ	128 MB	10 GB	10/100
SUN	Ultra 10	256 MB	20 GB	10/100
Windows Server	1.7 GHZ	512 MB	40 GB	10/100

LEGEND:
GHZ – Gigahertz
HP – Hewlett Packard
MAC – Macintosh
MB – Megabyte
NT – New Technology
PKI – Public Key Infrastructure
SP – Service Pack
UX – UNIX

APPENDIX C

REFERENCES

DEPARTMENT OF DEFENSE (DOD) DOCUMENTS

Joint Chiefs of Staff Publication 3-13, Joint Doctrine for Information Operations, 28 January 1998.

DOD Instruction 5200.40, DOD Information Technology Security Certification and Accreditation Process, 30 December 1997.

DOD Directive (DODD) S-3600.1, Information Operations, 9 December 1996.

DODD 5200.28, Security Requirements for Automated Information Systems, 21 March 1988.

Joint Chiefs of Staff Instruction 6212.01B, interoperability and Supportability of National Security Systems, and Information Technology Systems, 8 May 2000.

DOD CAC Release 1.0 Middleware Requirements, Version 2.1, 5 December 2001 published by the Access Card Office.

Common Access Card Specifications Release 1.0 (Draft), Smart Card Senior Coordinating Group, 24 April 2000.

Common Access Card Release 1.0 Reader Specification, 25 September 2000.

DEFENSE INFORMATION SYSTEMS AGENCY (DISA) DOCUMENTS

DISA Field Security Office, Security Technical Implementation Guides, April 2000. **http://iase.disa.mil**

JOINT INTEROPERABILITY TEST COMMAND DOCUMENTS

JITC Information Assurance Laboratory Test Requirements Baseline and Test Case Database, April 2001.

COMPONENT <SERVICE> DOCUMENTS

Operational Requirements Document (ORD) for the Joint Smart Card, U.S. Navy (Draft), undated.

MISCELLANEOUS DOCUMENTS

The Common Criteria for Information Technology Security Evaluations Version 2.1, August 1999. **http://www.radium.ncsc.mil**

Industry Best Practices List: Internet Security Systems' X-Force. **http://xforce.iss.net**

Industry Best Practices List: System Administration, Networking, and Security. **http://www.sans.org/newlook/home.htm**

Mitre Common Vulnerabilities and Exposures, May 2001. **http://cve.mitre.org/**

APPENDIX D

TEST REPORT CARD

REQUIREMENT	MEASURE OF SUCCESS
MANDATORY	
1. Service Provider(s) shall use the system services provided by the ICC Resource Manager.	a. Shall successfully track installed IFDs and make this information accessible to other applications. b. Shall successfully track known ICC types, along with their associated SP and supported Interfaces, and make this information available to other applications. c. Shall successfully track ICC insertion and removal events to maintain accurate information on available ICCs within the IFDs. d. Shall successfully control the allocation of IFD resources. e. Shall successfully support transaction primitives on access to services available within a given ICC
2. Service Provider modules are denoted as the CAC Cryptographic Middleware and CAC DoD Data Middleware.	They shall support the following: a. CAC Cryptographic Middleware: 1. Shall successfully support Digital Signature and Verification, 2. Shall successfully support Encryption and Decryption, 3. Shall successfully support Secure Authentication, & Certificate-Based Log-on b. CAC DoD Data API: 1. Shall successfully support the Read/Write function to DoD Data
3. The Middleware is required to provide bundled with the Cryptographic Middleware modules the capability for users to manage their CACs.	a. Shall provide an application or utility capable of viewing all PKI credentials on the CAC, registering PKI credentials within the client OS or browsers, and allowing user PIN changes.
4. The workstation resource utilization middleware module shall separately meet these requirements.	a. Shall assure the maximum disk space required for CAC middleware installation on a client workstation does not exceed 30 Mbytes and, for a server, shall not exceed 100 Mbytes. b. Shall assure the CAC middleware functions properly on a client workstation configuration equivalent to a 133 MHz minimum Pentium-compatible CPU with a minimum of 32 MB RAM. c. Shall assure when installed on a system equivalent to a 133 MHz Pen tium-compatible CPU with 32 Mbytes of RAM, the processing time consumed by the CAC Middleware does not exceed 10% (ten percent) of the overall time required for an application to access information on the CAC.

REQUIREMENT	MEASURE OF SUCCESS
5. Session Management is required to Maintain Best Practice	a. Shall successfully maintain the DoD vision that multiple 'middleware' products of varying functionality may be present on a single client at the same time. Therefore Middleware vendors are required to work in this environment and provide concise error handling in their middleware product. b. Shall successfully support these multi-vendor products operating in tandem. Vendors shall exhibit care when caching data on the client to prevent errors or properly handle error returns. c. All external user interface processes of supplied Middleware modules shall be compatible with, support, and not interfere with the accessibility (FAR subpart 39.2) features of the operating system in which they are installed.
6. The DoD is in process of registering Department specific Application Identifiers (AIDs) for all DoD owned and licensed applets. As an interim measure, middleware vendors must be aware that for some period there may be two AIDs for the same applet.	a. Shall successfully use the application information container, which contains the AIDs of all the applets on the card, as the first place the middleware should look on the card for the applet AIDs. An alternative would be for the middleware to read from configuration data to get the AIDs. b. Shall successfully support the ability for the middleware to handle these conditions since it is necessary for now until a firm distinction can be made between AIDs and the middleware that interacts with the applets.
7. As a matter of policy, the middleware will not be permitted to provide any additional crypto function or utility in the areas of initializing key material, injecting key material, re-keying, etc. The DoD reserves the right to provide the function of locking the card (upon three incorrect PIN entries) and unlocking the card at the RAPIDS stations.	a. Shall successfully implement both Public Key Cryptography Standards (PKCS #11) and Microsoft Cryptographic Service Provider (CSP). This can be implemented within single or separate modules. 1. The PKCS#11 (CSP) implementation shall support all the calls required to support the following mechanisms: a. RSA mechanisms (12.1) b. DSA mechanisms (12.2) c. Triple-Length DES (12.19) d. SHA-1 mechanisms (12.26) * All CALLs as part of all functions for the above mechanisms must be supported. 2. The Microsoft CryptoAPI (CSP) implementation shall support all the APIs defined in the following groups: Base Cryptography functions a. Certificate & certificate store functions b. Certificate verification functions c. Auxiliary functions • Data management functions • Data Conversions functions • OID functions * All CALLs are to be supported for all the above functions. b. Shall successfully implement modules in accordance with the "CAC Developer's Kit v2.0" c. Shall successfully implement utilizing the cryptographic services defined in the "CAC Developer's Kit v2.0

REQUIREMENT	MEASURE OF SUCCESS
	d. Shall successfully operate with PS/SC smart card readers and driver components for all devices. Optionally, it shall operate with PC/SC (M.U.S.C.L.E) and OCF smart card readers and driver components for Java OS, Unix, Linux, and Macintosh operating environments e. Shall successfully implement secure channel in accordance with Global Platform 2.0 or higher f. Shall be able to handle multiple context or sessions within the same module in accordance with Requirement 6. Specifically it shall: Provide services to insure that an application's transaction sequence with the CAC is not disrupted by other applications running on the user's workstation. These services are typically provided by LOCK and UNLOCK functions that can be utilized by a calling application to prevent other applications from making calls to the card that might change the currently selected applet or the values of card internal data. Upper middleware layers (like the PKCS #11 and MS CSP layers) must insure that applications do not abnormally terminate when calls are made that find the card to be unavailable because of another application's use of the LOCK functionality. g. Shall provide single sign-on support for smart card PIN verification by middleware. Prior to requesting a PIN from the user, the middleware must first perform the VerifyPIN command to the card with no PIN data to check if the PIN has already been verified. It is recognized that this requirement will not guarantee single sign-on functionality as an application may prompt the user for a PIN before interacting with the middleware.
8. The CAC cryptographic middleware will have bundled with it a client workstation application or utility capable of managing the CAC.	a. Shall have the capability to manage the card by: 1. Displaying (read only – PIN not required) the utility version number. 2. Requiring PIN entry to access any services from the card except for card identification information 3. Allowing the user the capability to change their PIN. 4. The Cryptographic Middleware may provide a PIN CHANGE UTILITY. However, the utility will be required to enforce the DoD PIN Policy of a six to eight digit numeric PIN. Utility will allow the user to change his PIN by submitting his current PIN and then providing a new PIN. Note that any resulting PIN must be in a six to eight digit numeric format. 5. Not allowing user any other write access to the card b. Shall have the capability to manage the card's certificates. It shall: 1. Require PIN entry to access any service from the card except for card identification information a. Provide for migration, display (read only), and deletion of certificates (and pointers to keys) to program's registry, client browser, client messaging system, or operating system on the client workstation 2. Display (read only) a list of certificates on the card, including unique name and expiration date. a. Display (read only) certificate data. c. Shall have the capability to manage the cryptographic middleware. It shall: 1. Display (read only – PIN not required) the middleware version number.

REQUIREMENT	MEASURE OF SUCCESS
	2. Have the capability to manage parameters (if any) required by the middleware – PIN not required, e.g., a. Port assignments for the reader b. Timeout periods. e. Shall have the capability to display help information. It shall: 1. Provide a description of all functions, from a user standpoint, provided by the utility. 2. Provide a description of all functions, from a user standpoint, provided by the middleware. 3. Provide a trouble shooting tutorial from a user standpoint.
9. This module provides the necessary "glue" to get the DoD data elements residing on the CAC to operate. It is responsible for exposing high-level interfaces to *non-cryptographic* services that include common interfaces to a CAC as well as access to file and authentication services.	a. Shall successfully be implemented in accordance with PC/SC and/or OCF for service providers b. Shall successfully implement modules in accordance with the "CAC Developer's Kit v2.0" c. Shall successfully implement utilizing the generic container API defined in the "CAC Developer's Kit v2.0" d. Shall successfully operate with PC/SC smart card readers and driver components for all devices. Optionally, it shall operate with PC/SC (M.U.S.C.L.E) and OCF smart card readers and driver components for Java OS, Unix, Linux, and Macintosh operating environments e. Shall successfully be able to handle multiple context or sessions within the same module in accordance with requirement 6. Specifically it shall: Provide services to insure that an application's transaction sequence with the CAC is not disrupted by other applications running on the user's workstation. These services are typically provided by LOCK and UNLOCK functions that can be utilized by a calling application to prevent other applications from making calls to the card that might change the currently selected applet or the values of card internal data. Upper middleware layers must insure that applications do not abnormally terminate when calls are made that find the card to be unavailable because of another application's use of the LOCK functionality.
10. A list of targeted platforms to be supported by CAC Release 1.0 middleware: Note: The middleware product must clearly identify which operating system it supports. A middleware product may support one or more of these platform, but is not required to support all operating systems.	Windows 95b Windows NT 4.0 (beginning with native mode SP 4) or higher Windows 2000 Linux 6.0 (or greater) HP-UX 11.x-12.x Solaris 2.51, 2.6, 7, and 8 RedHat Linux 6.2 MAC OS 8.0 (or greater)

NOTE: The procurement will be executed under the auspices of the DoD Enterprise Software Initiative (ESI) to establish an Enterprise Software Agreement for use by all Services and Components within DoD.
Test card issuance is accomplished via the DoD Real Time Automated Personnel Identification System (RAPIDS).